Technical Report 08-03
March 2008

Privacy Concerns Related to the Collection of Personal Information Under the Personal Identity Verification (PIV) Program

Whitney B. Helton-Fauth
Fauth Consulting

Approved for Public Distribution: Distribution Unlimited
Defense Personnel Security Research Center

Technical Report 08-03 **March 2008**

Privacy Concerns Related to the Collection of Personal Information Under the Personal Identity Verification (PIV) Program

Whitney B. Helton-Fauth, *Fauth Consulting*

Released By – James A. Riedel

BACKGROUND

With Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, the President mandated that all persons who require access to federally controlled facilities and information systems must apply for a Common Access Card (CAC) and undergo a background investigation. This necessarily requires the collection of various types of personal, and sometimes private, information from all applicants—information some may be reluctant to provide. Therefore, it is essential to identify possible concerns those persons subject to this policy may have regarding their personal privacy. It is equally important to acknowledge policy established by the federal government to safeguard personal information, and to ensure all individuals affected by HSPD-12 are aware of these safeguards.

HIGHLIGHTS

Personal privacy is highly valued in our society. New federal policies, such as Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, will require all persons who require ongoing access to federally controlled facilities and information systems undergo background investigations. There is some concern that anxiety about infringements on personal privacy may lead to reluctance to provide important information during these investigations, and it is our hope that such anxiety can be alleviated before personal information is collected. Therefore, this report outlines existing laws intended to protect personal privacy and details known privacy concerns related to the collection of personal information. In addition, we specify how existing federal policy, established to protect personal privacy, may mitigate these concerns and, where appropriate, we have provided suggestions for alleviating concerns that are not sufficiently addressed by existing policy.

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE

REPORT DOCUMENTATION PAGE	**Form Approved OMB No. 0704-0188**

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE: (04-03-2008)	2. REPORT TYPE Technical Report 08-03	3. DATES COVERED March 2005 – January 2006
4. Privacy Concerns Related to the Collection of Personal Information Under the Personal Identity Verification (PIV) Program	5a. CONTRACT NUMBER: NBCHD030003	
	5b. GRANT NUMBER:	
	5c. PROGRAM ELEMENT NUMBER:	
6. AUTHOR(S) Whitney B. Helton-Fauth	5d. PROJECT NUMBER:	
	5e. TASK NUMBER:	
	5f. WORK UNIT NUMBER:	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: Technical Report 08-03	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	10. SPONSORING/MONITOR'S ACRONYM(S): PERSEREC	
	11. SPONSORING/MONITOR'S REPORT NUMBER(S):	
12. DISTRIBUTION/AVAILABILITY STATEMENT: Distribution Unlimited		
13. SUPPLEMENTARY NOTES:		

14. ABSTRACT:

In any system that requires the collection of personally identifying information, privacy concerns arise that must be addressed prior to the implementation of the system. Therefore, this report attempts to: (1) identify known privacy concerns related to the collection of personal information and the causes for concerns; (2) identify federal policy in place that may help mitigate these concerns; and (3) provide recommendations for alleviating privacy concerns that are not sufficiently addressed by existing policy or FIPS 201.

15. SUBJECT TERMS: Personal Privacy, Privacy Concerns, Privacy Act, Personal Information, Personal Identity Verification

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT:	18. NUMBER OF PAGES: 67	19a. NAME OF RESPONSIBLE PERSON: James A. Riedel, Director
a. REPORT: UNCLASSIFIED	b. ABSTRACT: UNCLASSIFIED	c. THIS PAGE: UNCLASSIFIED			19b. TELEPHONE NUMBER (Include area code): 831-657-3000

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

PREFACE

The Defense Personnel Security Research Center (PERSEREC) was tasked by the Security Directorate within the DUSD (CI&S) to explore options to meet requirements for federal identification credentials (Common Access Cards) as required by Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, and specified in Federal Information Processing Standards Publication 201 (FIPS 201). Specifically, all persons applying for access credentials for federally controlled facilities and information systems must undergo a background investigation. Accordingly, applicants will be required to provide various types of personally identifying information. In any system that requires the collection of personally identifying information, including but not limited to full name and aliases, date of birth, home address, Social Security number, or biometric information, privacy concerns arise that must be addressed prior to the implementation of the system.

This study attempted to identify any possible privacy concerns that could arise during the course of the application process or background investigation. The study was not designed to measure the prevalence of any particular privacy concern, but rather to understand how differently people can think about these issues. Therefore, if written evidence of a privacy concern was discovered, it was considered a potential concern in the implementation of FIPS 201.

This report is being released in tandem with *FIPS 201 Part I: Identity Proofing Implementation Options* in order to promote fair and efficient implementation of the federal Personal Identity Verification (PIV) program detailed in HSPD-12 and FIPS 201.

James A. Riedel
Director

EXECUTIVE SUMMARY

With Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, the President mandated that all persons who require access to federally controlled facilities and information systems must apply for a Common Access Card (CAC) and undergo a background investigation. This necessarily requires the collection of various types of personal information from all applicants. Therefore, the purpose of this report is to: (1) outline existing laws intended to protect personal privacy; (2) detail known privacy concerns related to the collection of personal information, along with causes for these concerns; (3) specify how existing federal policy may mitigate these concerns; and (4) where appropriate, provide suggestions for alleviating concerns that are not sufficiently addressed by existing policy.

The legal definition of personal privacy is "freedom from unauthorized intrusion; a state of being let alone and able to keep certain, especially personal matters, to oneself." For individual Americans, however, privacy is not quite so easily defined. It is a personal, subjective condition, one that may be different for every person.

Whatever it is, Americans value privacy, and we may guard ourselves more carefully when we feel as if our privacy is being violated. In the legal system, there are three primary ways privacy of the average American citizen can be violated: (1) public disclosure of private or embarrassing facts; (2) false light, or negatively portraying a person as someone he or she is not; and (3) intrusion into someone's personal space, including trespassing and secret surveillance from an unauthorized agency. In everyday life, however, the precise definition of what constitutes an invasion of privacy may vary from one individual to the next; people may only be able to say that "they know it when they see it."

Recently, growing concern over how private, personal information such as name, date of birth, Social Security number, or biometric information is bought, sold, stolen, given away, and subsequently used in the United States and around the world has led to an increased awareness among Americans regarding (1) to whom that information is provided and (2) how that information will be used. This increasing wariness to provide personal information pertains not only to business and retail activities but also to how such information is obtained and maintained by government agencies.

An extensive review and analysis of existing privacy concerns revealed that a reluctance to provide personal information to government agencies may be motivated by two different types of personal privacy concerns. First, privacy concerns may be based on personal beliefs and values. These concerns are supported primarily by how people feel, what their "gut" tells them, and personal beliefs as to what will happen if they give away too much personal information. Such concerns are driven by fear and suspicion, and may be difficult to alleviate

with even the most logical explanations. Although these concerns may not be understood by some, they are important to those who have them.

Value-based privacy concerns center primarily on insecurity and lack of trust in government officials and operations. These may include:

- Lack of trust that the government will collect and use personal information for the specific purposes it has stated;
- Insecurity regarding current and emerging technologies (such as biometrics) about which an individual may know or understand little;
- Fear that the government will gather and use personal information for sinister purposes; and
- Belief that personal information is simply not the government's business.

A second type of privacy concerns are those based on reason. These concerns are based primarily on personal experience, word-of-mouth warnings, reasonable fears, media hype and history. They are driven by both realistic and unrealistic beliefs about the probability that personally identifying information, including biometric identifiers, will be misused, divulged to an unauthorized party, or otherwise be left unprotected. These may include:

- Concerns that information will be sold or otherwise provided to third-party agencies and other companies;
- Concerns that background investigations and information revealed during the course of investigation may unfairly affect personal and professional relationships;
- Concerns that personally identifying information provided to and stored in government databases will be vulnerable to theft and abuse; and
- Concerns that the collection and use of biometric identifiers will not be conducted appropriately.

The majority of reason-based concerns have only been exacerbated by the significant increase of identity theft cases in the last several years. Most of these concerns can be mitigated if applicants feel confident that the government is taking every precaution to protect their personal information from outsiders and to ensure that information is only used for the purposes specifically stated at the time of collection.

The federal government has been concerned about individual privacy rights for decades. The Privacy Act of 1974 is the core legislation for securing the privacy of Americans' personally identifying information. It regulates the collection, storage, use, and dissemination of personal information by federal agencies. The Computer Matching and Privacy Protection Act of 1989 amended the Privacy Act to ensure safety of personal information during the electronic transmission of data among federal agencies.

In addition to the Privacy Act, the E-Government Act of 2002 addresses the security of electronic data systems, including those containing personal information. The most important provision of the E-government Act may be that it requires federal agencies to conduct a Privacy Impact Assessment (PIA) prior to the establishment of any data system that will house personal information or prior to any change of an existing database that houses personal information. With respect to personally identifying information, the PIA requires agencies to identify (1) all current and expected uses of information; (2) why information is required; (3) individuals who will have access to information and how it will be handled (and adherence to all legal requirements); (4) any and all risks associated with the collection and storage of information; and (5) a privacy policy specific to the electronic database. The PIA must also provide information about opt-out and disclosure rules.

The Personal Identity Verification (PIV) Program is the large-scale federal identity proofing plan described in HSPD-12 and FIPS 201. In each federal agency, federal employees and contractors will be required to provide sufficient evidence of their identity, undergo a background investigation, and carry a CAC card that will verify their identity upon access to facilities and information systems. The PIV program in each federal agency, as directed in HSPD-12 and FIPS 201, is to follow the "letter and spirit" of the Privacy and E-Government Acts. While FIPS 201 does address several privacy issues, it fails to address all potential privacy concerns. In light of existing concerns and the absence of policy to fully alleviate them, suggestions have been presented for agencies to consider during the implementation of the PIV program. The following represent a summary of the various considerations detailed in this report:

- Information Security: All agencies should (1) take all possible steps to protect personal information from unauthorized access, and (2) ensure that all PIV applicants fully understand their rights under the Privacy and E-Government Acts.
- Collection of Biometric Identifiers: All government agencies should take every step necessary to (1) ensure biometric information is collected in the most humane manner possible, and (2) protect biometric information from unauthorized access.
- Third-Party Access to Personal Information: All agencies should establish policies that hold third parties responsible for following the letter of the law in protecting personal information.
- Background Investigations: In the conduct of background investigations, all agencies should take every step necessary to (1) establish guidelines for collecting and evaluating personal information, including guidelines for using external sources (such as data brokers) to gather information, and (2) investigators and adjudicators must take every precaution to protect applicants' personal information throughout the course of the investigation.

TABLE OF CONTENTS

INTRODUCTION

Americans value privacy. Because it is so important, we may guard ourselves more carefully when we feel as though our privacy is being violated. In the legal system, there are three primary ways the privacy of the average American citizen can be violated: (1) public disclosure of private or embarrassing facts; (2) false light, or negatively portraying a person as someone he or she is not; and (3) intrusion into someone's personal space, including trespassing and secret surveillance from an unauthorized agency (Student Press Law Center, 2001). In everyday life, however, the precise definition of what constitutes an invasion of privacy may vary from one individual to the next; most people will simply say they "know it when they see it."

Recently, growing concern over how private, personal information is bought, sold, stolen, given away, and subsequently used in the United States and around the world has led to an increased awareness among Americans regarding (1) to whom that information is provided and (2) how that information will be used. This increasing wariness to provide personal information pertains not only to business and retail activities, but also to how personal information is obtained and maintained by government agencies.

The President has mandated that all persons who receive credentials for access to federally controlled facilities and information systems must undergo a background investigation (Bush, 2004). This necessarily requires the collection of various types of personal information from all persons who apply for access to federal properties on a regular basis. Therefore, the purpose of this report is to: (1) outline existing laws intended to protect personal privacy; (2) detail known privacy concerns related to the collection of personal information along with causes for these concerns; (3) specify how existing federal policy may mitigate these concerns; and (4) where appropriate, provide suggestions for alleviating concerns that are not sufficiently addressed by existing policy.

FEDERAL PRIVACY POLICIES

The federal government is aware that privacy is highly valued among the American people. For decades, the government has attempted to ensure that the privacy of the common citizen be protected from both the government and from criminals who wish to use another's personal information for insidious purposes. The most commonly referenced privacy legislations are the Privacy Act of 1974 (as amended) and the E-Government Act of 2002.

Privacy Act of 1974

The Privacy Act of 1974 was the first formal attempt at securing the privacy of Americans' personally identifying information (U.S. Department of Justice, 2004a; 2004b). It was created to regulate the collection, storage, use, and dissemination of

personal information by federal agencies. The Computer Matching and Privacy Protection Act of 1989 amended the Privacy Act to ensure safety of personal information during the electronic transmission of data between federal agencies. The Privacy Act is intended to protect the privacy of the American public by:

- Requiring full and public disclosure if and when personal information will be used for a purpose other than that for which it was originally collected;
- With exceptions, requiring that an agency obtain written permission from an individual before sharing his or her personal information with anyone other person or agency;
- Requiring Congressional approval before databases containing personal information can be linked to another database (shared with another agency);
- Requiring agencies to keep accurate accounts of when and to whom personal records are disclosed (with the exception of disclosures to law enforcement);
- Requiring agencies to collect the minimal amount of personal information that is "relevant and necessary" to accomplish the stated purpose;
- Requiring an agency to collect as much information as possible from the individual (as opposed to gathering data from other sources);
- Requiring that individuals have access to any records that agencies have about them;
- Requiring an appeals process if an applicant wishes to change or deny any information contained in a record;
- Providing for civil and criminal penalties for individuals and agencies who violate its provisions; and
- Requiring that agency personnel who have access to personal information receive at least biannual training on Privacy Act provisions.

E-Government Act of 2002

The E-Government Act of 2002 addresses the security of electronic data systems, including those containing personal information. The most important provision of the E-Government Act may be that it requires federal agencies to conduct a Privacy Impact Assessment (PIA)[1] prior to the establishment of any data system that will house personal information or prior to any change of an existing database that houses personal information. With respect to personally identifying information, the PIA requires agencies to identify (1) all current and expected uses of information; (2) why information is needed; (3) who will have access to information and how it will be handled (and adherence to all legal requirements); (4) any and all risks associated with the collection and storage of information; and (5) a privacy policy

[1] For more information, see OMB M-03-22, Attachment A, Section II: Privacy Impact Assessment, http://www.whitehouse.gov/omb/memoranda/m03-22.html#5. Examples of existing PIAs can be found online at http://www.ftc.gov/os/2004/11/041104coninfosysprivimpassess.pdf or http://www.dimhrs.mil/LeftMenuBar/InformationCenter/DIMHRS_PIA%20v2.4.pdf.

specific to the electronic database. The PIA must also provide information about opt-out and disclosure rules. The primary privacy provisions of the E-Government Act of 2002 are as follows:

- Agencies are required to conduct a PIA:
  - When a database containing personal information is created or modified, and
  - Biannually so long as the database remains the same;
- Agencies are required to make the PIA available to the general public;
- Agencies are required to post privacy policies whenever personal information is electronically collected or stored; the policies must address the nature, purpose, use and potential sharing of collected information; and
- All agencies must provide an annual report to the Office of Management and Budget (OMB), the federal oversight agency for privacy matters.

Privacy Provisions of the Personnel Identity Verification Program

The implementation of the Personnel Identity Verification (PIV) program in each federal agency, as directed in Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standards 201 (FIPS 201), is to follow the "letter and spirit" of these laws (Bush, 2004; U.S. Department of Commerce, 2005). Specifically, Section 2.4 of FIPS 201 mandates the following to ensure the privacy of applicants:

- Assign a senior agency official in each agency to oversee privacy-related matters in the PIV system.
- Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information for the purpose of implementing PIV.
- Write, publish, and maintain a clear and comprehensive document listing the types of personal information that will be collected for the PIV program. This document should state the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and all uses of personal information at each agency.
- Assure that systems that contain personal information for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices according to the Privacy Act.
- Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.
- Ensure that only personnel with a legitimate need for access to personal information in the PIV system are authorized to access such.
- Each agency should define consequences for violating privacy policies of the PIV system.

- Assure that the technologies used in each agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.
- Use appropriate security controls to protect personal information.
- Ensure that the technologies used to implement the PIV program sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in identifiable form (i.e., use electromagnetically opaque sleeves or other technology to protect against any unauthorized contactless access to information stored on a Common Access Card [CAC]).

TYPES OF PRIVACY CONCERNS

A reluctance to provide personal information to government agencies can represent two different types of personal privacy concerns. First, privacy concerns may be based on personal beliefs and values. These concerns are supported primarily by how people feel, what their "gut" tells them, and personal beliefs as to what will happen if they give away personal information. Such concerns are driven by fear and suspicion, and may be difficult to alleviate with even the most logical explanations. Although these concerns may not be understood by some, they are important to those who have them.

Other privacy concerns are based on reason. These concerns are based primarily on personal experience, word-of-mouth warnings, reasonable fears, media hype and history. They are driven by both realistic and unrealistic beliefs about the probability that personally identifying information, including biometric identifiers, will be misused, divulged to an unauthorized party, or otherwise left unprotected.

Although FIPS 201 carefully outlines privacy protections for the PIV program, it fails to address all of the privacy concerns that Americans may have. Therefore, this report attempts to (1) identify the different value- and reason-based concerns that Americans have about providing personal information to government agencies, and explain the causes for these concerns; (2) present facts regarding policy and intended scope of the PIV program that may work to mitigate these concerns; and (3) where appropriate, provide considerations for agencies, as they implement the PIV program, to help them address or alleviate concerns that are not sufficiently addressed by policy or FIPS 201. Each concern is organized according to primary concern, causes for the concern, facts regarding existing policy that are related to the concern, and suggestions for alleviating each concern that is not adequately addressed by current policy.

METHODS

The concerns cited in this report were obtained through an extensive review of the privacy literature. In order to identify specific privacy concerns related to the collection of personal information, we conducted a key-word search using Internet search engines such as Google, Yahoo!Search, and LexisNexis. Key-word searches were also conducted within specific privacy-related Internet sites such as the American Civil Liberties Union, the Electronic Privacy Information Center (EPIC), and the Privacy Rights Clearinghouse, and within several U.S. agency websites, including the Government Accountability Office (GAO), Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Defense (DoD), and Federal Trade Commission (FTC). Key-word searches were based on the following phrases or combination of phrases: privacy, invasion(s) of privacy, right(s) to privacy, privacy policy(ies), privacy protection(s), privacy objection(s), biometrics, surveillance, data mining, and data brokers.

Concerns identified as a result of this search were first compiled in a list, along with supporting causes for each and any related examples. They were then organized into categories based on their content (i.e., belief in the right to privacy, concerns about Social Security number (SSN) protection, or concerns about the use of brokered data, etc.), resulting in individual categories of concerns.

Next, concerns were separated into the two types described above: (1) those that are based on personal beliefs and values, and (2) those that are based on logic and reason. During the course of analyzing these concerns, it became obvious that most, if not all, contain some element of emotion for those who have them. There were specific categories, however, that appeared to be *driven* by emotion and based in personal beliefs and values. These categories include fears that cannot be adequately alleviated using logical, reason-based information. People who had these concerns were not always able to fully describe the reasons behind them; they may not be able to explain specifically *how* their rights might be being violated, but they feel that something isn't right.

Other concerns were based more on specific information or reason. People had experienced personal problems after providing personal information or knew someone who had; they watched news reports on potential problems with certain information systems; they were aware of the real risks of identity theft. These concerns were formed in the interest of protecting personal information to reduce risk or avoid harm, and can be alleviated by providing ample information regarding rules, laws, and other measures intended to protect people who disclose their personal information.

The concerns presented here do not necessarily represent the opinions of the author, nor do they necessarily represent the majority of CAC applicants. Rather, they are intended to reflect the actual tone of the privacy concerns expressed by

privacy advocates and American people. Accordingly, causes for concerns are intended to reflect the information, beliefs and fears, whether accurate or not, that have led individuals to experience fear or anxiety about providing personal information. It should be noted that we were asked to identify all possible privacy concerns, not just those voiced by the American majority or by federal employees and contractors. Therefore, if during the course of our investigation we found written evidence that an American or any group of Americans had voiced a specific privacy concern, that concern was included in this report.

VALUE-BASED CONCERNS

CONCERN: LACK OF TRUST IN GOVERNMENT

- I don't trust the government with my information.
- Providing information to the government makes me nervous.
- The database that is created to store this personal information will evolve to the point where it is abused; it will lead to greater infringement on my personal rights.
- I am concerned that the government will use this information for purposes other than that for which it is initially collected.

Cause for Concern

Some Americans do not trust the U.S. government. Lack of trust may be driven by the belief that the government may not do what they say they will or they change rules relevant to immediate need; they exempt organizations that find it difficult to comply with the law or because compliance would cost too much.

Privacy advocates are concerned that data initially collected to verify identity upon access to federal facilities under the Personal Identity Verification (PIV) program will eventually be used for different (or unauthorized) identity verification purposes such as government monitoring, as a basis for a "full-fledged National ID system," or for linking and integrating the various ID card/credential databases maintained by state and federal agencies. Privacy advocates are also concerned that the public draft of FIPS 201 contains no discussion of controlling and limiting the use of the "credential identifier" (the unique user identification number). This raises concerns about future use of such a serial number. Advocates are concerned that, if not tightly controlled, the number will eventually be accepted as a federal proof of ID for any number of purposes (banking, shopping, establishing utility services, etc.), making it yet another target for identity thieves.

Example: SSNs were originally promised to be used for administration of a federal retirement program only. Eventually, Congress allowed the Internal Revenue Service (IRS) to use them for certain tax purposes and they soon became a universal identifier. For decades, the SSN was routinely used as the common ID number on drivers' licenses, student IDs, and employee IDs. The SSN is readily accepted as a valid identifier for individuals who are writing checks or applying for credit, and it is very often used as the primary identification number for criminal records, educational records, and insurance policies. Accordingly, the SSN is also frequently used as the primary key or code for storing and retrieving personal information. Because it is possible to access an abundance of information about people knowing only their name and SSN, the SSN is commonly used by the

government and law enforcement to locate people. Unfortunately, it is also considered a prize for identity thieves.

Mitigating Facts

- The Privacy Act and E-Government Act were enacted to protect the privacy of Americans. Agencies collecting personal information are required to satisfy the privacy and security requirements of both Acts prior to the collection of information.
- The Privacy Act:
  - Requires full and public disclosure if and when personal information will be used for a purpose other than that for which it was originally collected.
  - Requires that an agency obtain written permission from an applicant before sharing his or her personal information with anyone else.
    - Exceptions to this requirement include providing information:
      - To employees of the sponsoring agency who have a need to know under the Freedom of Information Act
      - For routine uses (those for which information was originally collected)
      - To the Census Bureau
      - For statistical research
      - To the National Archives for historical value
      - To law enforcement
      - When there are "compelling circumstances" affecting someone's health and safety
      - To Congress
      - To the Comptroller General
      - Pursuant to a court order
      - To a consumer reporting agency in accordance with 31 U.S. C. 3711(e)[2]
    - With all of the above-listed exceptions, there still must be a legitimate need to know before personal information is shared with another party.
      - Requires Congressional approval before databases containing personal information can be linked to another database (shared with another agency).
- The E-Government Act of 2002 requires federal agencies to conduct a Privacy Impact Assessment (PIA) prior to the establishment of any data system that will

[2] Information may be provided to a consumer reporting agency when an executive, judicial, or legislative agency has a legitimate outstanding claim against an individual.

house personal information or prior to any change of an existing database. The PIA requires agencies to identify (1) all current and expected uses of information; (2) why information is needed; (3) who will have access to information and how it will be handled (and adherence to all legal requirements); (4) any and all risks associated with the collection and storage of information; and (5) a privacy policy specific to the electronic database. The PIA must also provide information about opt-out and disclosure rules.

- HSPD-12 & FIPS 201 require all agencies to implement the PIV program in accordance with the "spirit and letter" of all privacy controls set forth in the Privacy and E-Government Acts.
- FIPS 201 requires all agencies to "write, publish, and maintain a *clear and comprehensive* document listing the types of information that will be collected, the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. PIV applicants shall be provided full disclosure of the intended uses of the PIV credential and the related privacy implications."

Considerations for Implementation of PIV

- Establish procedures for obtaining written consent from all applicants prior to the collection of any personal information.
- Reinforce that the PIV program is intended to be used to authenticate identification prior to and upon access to federal facilities; it will not be used to create a "national" database to house information on all Americans.
- If a unique cardholder identification number will be assigned to each individual holding a credential, reinforce the fact that unique identification numbers assigned through the PIV program will be used only for the PIV program.

CONCERN: RIGHT TO PRIVACY

- I have a constitutional right to control and protect my personal information.
- The United States has fewer privacy laws than other countries. If the European Union (EU) won't provide its citizens' personal information to the U.S. government due to lack of privacy laws, why should I?
- I have a moral or religious objection to providing personal information.
- I have a right to be left alone.

Cause for Concern

In the United States we have an expected right to privacy. Merriam-Webster defines privacy as "freedom from unauthorized intrusion; [a] state of being let alone and able to keep certain, especially personal matters, to oneself." Some Americans fear that if we give up more and more of that privacy we will eventually turn into a society where we have no privacy at all and the government will control all aspects

of our lives. Extended monitoring based on electronic information storage has led to a point where some fear that the government can find out practically anything at all about us.

Example: During an independent council's investigation of the actions of former President Clinton, Monica Lewinsky's credit card records were subpoenaed by Ken Starr in an effort to track book purchases she made at a book store. He was able to learn exactly what purchases were made at a particular book retailer. There is no reason that similar information would not be available for every other American.

Example: Government and law enforcement agencies are routinely exempt from privacy provisions imposed on other third-party entities (such as marketers or other businesses). Citibank and MNBA, for example, both specifically state in their privacy policies that all personal information contained in their records is revealed to government agencies upon subpoena or as required by law. "As required by law" is not specifically defined in either of the policies, and may lead agencies to provide personal information to government officials without questioning their true need to know.

Mitigating Facts

- The U.S. government agrees that individual right to privacy must be protected. The Privacy Act was written, and has been amended as technology changes, to ensure personal privacy for Americans.
- The U.S. Constitution protects against unreasonable searches and seizures. In most cases, officials must have a probable cause to investigate a person without that person's knowledge or consent.
- An applicant must consent to providing personal information and to the background check to ensure he or she does not constitute a threat to national security upon access to federal facilities.
    - Exceptions to this rule exist under the PATRIOT Act. When dealing with suspected "domestic" terrorists, federal agents have the right to:
        - Conduct surveillance and searches against U.S. citizens without "probable cause;" the suspect is not notified and cannot challenge the action;
        - Conduct "sneak-and-peek" searches without prior notice in common domestic crime investigations; and
        - Access any person's business or personal records.
- All Americans have the right to "opt out" of providing their personal information. Businesses and government also have the right to refuse service (in the present case, access to facilities) to those not willing to provide information upon request.
- The United States does, in fact, have an agreement to share personal information between U.S. and EU entities.

- The EU approved this program, known as "Safe Harbour," in 2000.
- Safe Harbour requires U.S. organizations, both public and private, that wish to compile data on EU customers or clients to:
  - Notify individuals when their personal information will be used or stored;
  - Give applicants the opportunity to choose whether their personal information can be shared with third parties;
  - Ensure that all third parties also subscribe to Safe Harbour mandates;
  - Provide applicants access to their personal information;
  - Maintain adequate data security and quality control measures; and
  - Provide independent audits and investigations should concerns arise.
- Safe Harbour applies to how U.S. companies use and store information on European customers only; it does not address how U.S. companies use and store information on U.S. customers.

Considerations for Implementation

- Reinforce the idea that the government is a better protector of personal information than almost any other entity:
  - According to the Privacy Act, the government is required to obtain approval and notify an individual every time his or her information is provided to an outside party. Retailers and other business entities are only required to provide an opt-out at the individual's request and a once-per-year statement of how information is, or might possibly be, used.
  - Any people who apply for and use store loyalty cards make their personal information available to the store and to mass marketers, who can easily track every purchase made.
  - Even for those who refuse store loyalty cards for the above-mentioned reasons, anyone who regularly pays for purchases with a debit, check, or credit card allows every purchase to be tracked.
  - Any individual who has ever been subject to a court hearing has, at a minimum, his or her name and address on file for the public to access in the form of public records unless they have requested redaction.
  - All of this information has likely been compiled and stored in a single file by one of the many data brokers in existence. These brokers are not required to check for accuracy or timeliness of information before they sell it to a customer.

CONCERN: OBJECTION TO THE COLLECTION OF BIOMETRIC IDENTIFIERS

- If the government collects my biometric information, I will never have privacy again.

- I don't want the government to store biometric information because they will be able to use it to track my comings and goings.
- The collection of my biometric information is a serious, intentional, and degrading violation of my physical person.
- The government will collect my fingerprints and use them in future criminal investigations.
- I have a religious objection to providing my biometric identifiers.

Cause for Concern

The collection of biometric information such as facial images, iris scans, fingerprints, or DNA "unquestionably" ties a person to his or her chosen identification. Once biometric information is collected on a person, there is essentially no way to maintain anonymity. Some Americans fear that if the government has access to such information they will never again be able to do things privately. There is fear that simply being in a place where a crime occurs will make them a suspect. They fear that the government will use biometric information to monitor their activities, to surreptitiously follow them as they move throughout their lives.

Example: Parent and grandparent volunteers in a school district in North Carolina feel they were "bullied" into providing their fingerprints after a child molester was found to be working in the system (Ritchey, 2002). The volunteers argued that the printing was an inherent violation of their personal privacy, and the school administration was using it as a "catch all" tool after their frightening experience. The school board told volunteers that, unless they provided fingerprints, they would not be allowed to work at the school. Volunteers even presented data that showed that the 70- and 80-year-old volunteers were not a "clear and present" danger to the children, and that a full-fledged fingerprinting sweep would not have identified the previously mentioned child molester. Several volunteers were outraged at what they felt was blackmail and one claimed that he would not "willingly submit [him]self to a witch hunt."

Biometrics not only provide information *about* a person, but *of*, or inherent to, the person. The collection of most biometric information necessarily involves physical contact with a person. Facial and iris scans may be uncomfortable. Fingerprinting often involves a trained printer who must firmly grasp the individual's wrist and finger and roll the finger on the collection media. DNA collection is by far the most intrusive, requiring collection of body fluids or body tissues.

Some religious groups have a deep-set objection to the collection of biometrics, calling them the "mark of the beast" as described in Revelation 13:16-17: "He also forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead, so that no one could buy or sell unless he had

the mark, which is the name of the beast or the number of his name."[3] Although this notion may not be understood by some, perceived violation of religious freedom is something that must be taken seriously.

Mitigating Facts

- Individuals have no right to anonymity upon access to federal facilities.
- In *Davis v. Mississippi* (1969) the Supreme Court ruled that the collection of fingerprints does not constitute an unreasonable search and that it "involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."
- Federal and state courts have ruled that the collection of fingerprints is not unconstitutional and is no more a violation of privacy than taking a photo or obtaining a signature.
- The collection and electronic storage of biometric identifiers is subject to the same laws and regulations as personal information; The Privacy Act and E-Government Act both govern the collection and storage of biometric information.
- Photos are a biometric that have had accepted use for decades. Fingerprints are simply another biometric, in addition to the photo.
- There are no plans to use biometric information for anything other than the purposes for which they are initially collected:
  - To authenticate an applicant's identity
  - To check that identity against local, state, and federal law enforcement databases
  - To personalize an employee's CAC
  - To electronically authenticate an individual's identity upon computer system, room, building, or facility access (comparison of fingerprints to those stored)
  - To manually authenticate an individual's identity upon computer system, room, building, or facility access (comparison of photo to face)
- At least one state court has ruled that it was not a violation of the state's constitution to compare fingerprints obtained in a criminal investigation to those obtained during employment screening.
- There are no plans to use biometrics to track "comings and goings" outside federal facilities. The biometrics embedded in the CAC will allow tracking when an individual enters a computer system, room, building or facility, similar to the way a security guard would observe people as they enter a building. Thus, if individuals attempt to enter a system to which they are not authorized, facility security will be notified.

[3] For one example see: http://www.rapturealert.com/052805evolutionmob.html

Considerations for Implementation

- When the collection of biometric information requires physical contact, make every effort to collect the information in a manner that is neither degrading nor humiliating to the applicant.
- Seriously consider religious objections to the collection and use of biometric information and work to formulate an approach for handling such cases.[4]
- Ensure that databases containing biometric information meet all E-Government requirements before they are linked to any other databases in local, state, or federal systems.
- Do not use DNA as a required biometric in order to avoid personally intrusive or embarrassing biometric collection procedures.
- Remind those with objections that biometrics, in the form of facial images on IDs, have been used for many years to verify identity (i.e., drivers' licenses, student IDs, employee IDs, etc.).
- Emphasize that applicants' consent is required to collect the biometric. Applicants are free not to provide biometric and other personally identifying information. It means they will have to forgo access to government facilities.

CONCERN: FEAR OF TOO MUCH GOVERNMENTAL CONTROL

- I am not willing to trade my liberty and freedom for unproven, increased safety measures.
- Providing my personal information violates my dignity, personal control, and political parity.
- The choice on whether to provide personal information should not be up to the government.
- The collection of my biometric information is equivalent to an unlawful and intrusive search of my person.
- The government isn't concerned about privacy, but about power and authority over Americans.
- Full disclosure of personal information will be used to ensnare innocent people.
- The government will misuse or abuse my personal information.
- I don't want to be assigned a unique identification number that can always be traced back to me.

[4] Unfortunately, the best way to handle religious objections to any government procedure appears to be on a case-by-case basis. In past cases of religious objections to government policy, the Supreme Court has consistently ruled in favor of the government so long as the free exercise of religion is not violated. For more information, see: http://www.churchstatelaw.com/casecategories.asp

Cause for Concern

> "*They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.*" —Benjamin Franklin

Some Americans fear that if too much information about their preferences and behaviors is available to government they will lose the right to be individuals, including their right to disagree with the government. Facial recognition, for example, can pick people out of crowds. Persons involved in a demonstration against the government are easily recognized. There are some who fear they will be penalized at a future time for expressing their disagreement with the government. This would be an obvious violation of freedom of speech.

People also fear that extensive monitoring will lead to government's intrusion into the most private aspects of their lives. Many people have extremely personal experiences or relationships that, if known, might subject them to harsher judgment from friends, family, and coworkers. Other people feel that personal relationships and personal behaviors, as long as they do not cause harm or violate the law, are simply not the government's business.

Mitigating Facts

- Americans do have a choice about providing personal information, but those who choose not to may be denied access to federal facilities because the government has little or no means of verifying whether or not they constitute a security risk.
- The collection of biometric information does not constitute an unreasonable search and seizure as defined by the 4th Amendment because applicants must consent to providing their biometric information.
- The government is, itself, controlled with regard to how it can use personal information. The Privacy Act and E-Government Act impart strict rules over the use, disclosure, and security of personal information.
- Under the Privacy Act, the government is not allowed to maintain any records "describing how an individual exercises rights guaranteed by the First Amendment" (i.e., participation in a political rally, participation in a picket against a government policy, publicly speaking out against an elected official, etc.) unless (1) an agency has been otherwise authorized by law to collect such information; (2) the applicant authorizes the collection of such information; or (3) the information is collected as part of an ongoing law enforcement investigation.
- The Privacy Act:
  - Requires that applicants have access to any records that agencies might have about them.
  - Requires an appeals process if an applicant wishes to change or deny any information contained in a record.

- Requires full disclosure as to why and for what specific purposes information is initially collected.
- Requires full and public disclosure if and when personal information will be used for a purpose other than that for which it was originally collected.
- Requires that an agency obtain written permission from applicants before sharing their personal information with anyone else.
- Requires agencies to keep accurate accounts of when and to whom personal records are disclosed (with the exception of disclosures to law enforcement).
- Requires agencies to collect the minimal amount of personal information that is "relevant and necessary" to accomplish the stated purpose.
- Requires an agency to collect as much information as possible from the applicant (as opposed to gathering data from other sources).
- Requires Congressional approval before databases containing personal information can be linked to another database (shared with another agency).
- Provides for civil and criminal penalties for individuals and agencies who violate Privacy Act provisions.
- Requires that agency personnel who have access to personal information receive at least biannual training on Privacy Act provisions.

- The E-Government Act:
  - Requires agencies to conduct a PIA (1) when a database is created or modified and (2) biannually so long as the database remains the same.
  - Requires the PIA to analyze and describe:
    - What information will be collected
    - Why information will be collected
    - How information will be used
    - With whom information will be shared
    - Opportunities for individuals to opt out
    - How information will be secured
    - If personal information will be collected (and therefore subject to the Privacy Act)
    - The consequences of collecting personal information
    - Any alternatives to collecting such information
    - Information "life cycle," including collection, use, retention, processing, disclosure, and destruction
  - Requires the PIA be made available to the general public.

- Requires agencies to post privacy policies whenever personal information is electronically collected or stored. Such policies must address the nature, purpose, use and sharing of collected information.
- Requires agencies to provide an annual report to OMB.

Considerations for Implementation

- Make every effort to ensure that the unique cardholder identification number is only linked to the federal credential system database and does not link to other, outside data systems.
- Ensure that database handlers and managers receive regular (annual or biannual) training on Privacy Act and E-Government Act requirements.

REASON-BASED CONCERNS

CONCERN: THIRD PARTY ACCESS TO PERSONAL INFORMATION

- Will my personal information be sold or provided to third parties who may or may not have a need to know?
- Will I be notified if my personal information will be provided to a third party?
- Will the government sell my personal information to marketing companies?
- Will my personal information be used to send me junk or unsolicited mail?
- Will my personal information be made available to outside parties who intend to do me harm?
- Will I be given the opportunity to opt out of my personal information being provided to third parties?
- What do data brokers do with my information when the government provides my personally identifying information in an attempt to gather information on me?

Cause for Concern

Businesses and financial institutions commonly share information with data brokers, mass marketers, and other businesses without prior consent from the individual. Americans want a guarantee that the government will not do the same thing.

Example: Orbitz.com provided personal information, name, address, and credit card information to an affiliate company, MWI*Connection, without the knowledge or consent of some customers. This type of data transfer or sell often results in unsolicited and unwanted junk mail or telemarketing, which some consider an invasion of privacy.

It is uncertain what happens to personal information provided to data brokers by the government during the execution of the security investigation. According to ChoicePoint, a national supplier of identification and credential verification data for local, state, and federal law enforcement and government agencies, customer-supplied data (data provided by the government when requesting an applicant's file) are stored separately from the files that ChoicePoint compiles and sells. However, the company does not specify if or when information is subsequently used to create new files or to supplement existing files.

Mitigating Facts

- The Privacy Act prohibits the sale or rental of personal information to third party marketers without the express written consent of the applicant.

- The Privacy Act allows for civil and criminal penalties to individuals or agents who violate disclosure regulations.
- Even when permission is granted, agencies are required to (1) maintain records detailing the date, nature, and purpose of each disclosure of a record to any person or agency; and (2) record the name and address of the person to whom the disclosure was made.
- Redisclosure of information is strictly prohibited, and any agency violating this is subject to penalty.

CONCERN: AGENCY SHARING OF PERSONAL INFORMATION

- Can agencies choose to share information if they find it useful?
- Will all federal agencies eventually be able to access personal identification information for every individual who has access to a federal facility?
- Will I have any say in when, with whom, and for what reasons my personal information is shared or provided to another government agency or agency representative?
- Will the more negative aspects of my life be shared with other agencies for other decisions about me?

Cause for Concern

Local, state, and federal agencies routinely share information. For example, local, state, and federal law enforcement agencies share information on suspects or known criminals with each other. With the passage of the REAL ID Act of 2005, all state Departments of Motor Vehicles (DMVs) were required to store, at a minimum, "all data fields printed on drivers' licenses and ID cards…and…motor vehicle histories" in an automated database that will be available to all other state DMVs and local, state, and federal law enforcement agencies (REAL ID Act, 2005). Additionally, this information will be shared with SSA for identity verification purposes.

Information sharing between agencies is often done in an attempt to verify identity and establish access to services or facilities. At other times, information is shared in order to reduce paperwork and to reduce the burden of data collection on individuals. Some Americans, however, feel that there is no justifiable reason for agencies to share information if it is not for routine "law enforcement" investigations. People want to be aware of who is accessing their personal information and for what reasons. They should be made aware of information sharing, even when there is a legitimate need to know.

Example: In a recent news report about government data mining and sharing, Senator Daniel Akaka, D-Hawaii, noted that Americans "would be surprised" if they knew how often government agencies shared data about citizens (Claburn, 2004).

Despite the Drivers' Privacy Protection Act[5] (DPPA), local, state, and federal authorities may still request driver information for legitimate government agency functions.

Mitigating Facts

- Agency sharing (sharing personal information collected and stored in one agency with another agency) is common in that it provides an important tool in promoting government efficiency. By sharing data, agencies can validate existing data, eliminate unnecessary paperwork, identify and prevent fraud, identify program beneficiaries, and reduce the public information collection burden.
- Agency sharing is subject to the data disclosure rules set forth in the Privacy Act.
- The Computer Matching and Privacy Protection Act, an amendment to the Privacy Act, governs how data are shared among government agencies.
- The Privacy Act requires Congressional approval before a database containing personal information can be linked to another database (shared with another agency).
- The Privacy Act requires written agreement authorizing data sharing between two government agencies or between a government agency and a federal contractor.
- OMB has set forth eight principles for conducting interagency data sharing based on existing requirements of the Privacy Act (U.S. Office of Management and Budget, 2000).
    - Notice
        - Agencies that plan to use data sharing must provide notice to affected individuals.
        - Agencies must publish notice in the Federal Register, at least 30 days prior to conducting the matching, describing the purpose of the match, records or individuals affected, and other relevant information.
    - Consent
        - Agencies should obtain written or electronic consent from applicants before sharing personal information, except in relation to exemptions detailed in Section 522a(b) of the Privacy Act (see *Lack of Trust in Government,* p. 7).
    - Redisclosure Limitations
        - Redisclosure by recipient agencies is prohibited except when required by law (such as in a criminal investigation) or to conduct the matching program.

[5] The DPPA prohibits the release and use of personal information from state motor vehicle records to any person or entity who does not have a legally specified need to know.

- Accuracy
  - Because information may be used in a way that can adversely affect a person, agencies must incorporate procedures to ensure the accuracy of data that are shared, including:
    - Allowing applicants to have access to their own data.
    - Allowing applicants to request amendment of their data.
  - Before an agency takes adverse action against an applicant based on information obtained through data sharing, it must independently verify such information before any adverse action is taken (except in cases where information is so sensitive as to constitute a security risk if it is revealed).
  - Agencies must provide notice to the applicant of the possibility of adverse action at least 30 days before the action is taken to give the applicant an opportunity to contest any findings.
- Security Controls
  - Agencies should employ "adequate and effective security controls to protect the confidentiality, availability, and integrity of all systems and data, including all data shared with other organizations."
  - Agencies must ensure recipient agencies have adequate security controls in place before the matching takes place.
  - The originating agency is ultimately responsible for physical and electronic data security.
- Minimization
  - Agencies should make a concerted effort to identify what data are needed for a specific purpose and make every effort to ensure that only those data are shared. For example, if an agency is attempting to verify identity through a shared database, the only information to be shared would be identity information, such as fingerprint scans, SSN, and aliases. Information about personal preferences, behaviors, or criminal history should not be shared.
- Accountability
  - Agencies are encouraged to promote accountability throughout the organization.
  - Agencies can be held civilly and criminally accountable for violating the mandates of the Privacy Act.
- Privacy Impact Assessments should be routinely conducted and published for data matching programs.

Considerations for Implementation

- Closely monitor agency sharing of personal information collected and stored under the auspices of the PIV Program.
    - Compare information provided by and collected from applicants with other agencies' databases only as specified in the PIA (i.e., Driver's license number will be checked against state motor vehicle agencies, and fingerprints will be compared to those maintained in the FBI's crime database).
    - If possible, allow the PIV Program database to "link" (permanently connect and access) to other relevant databases, but prevent other agency databases from linking to the PIV database. In other words, the PIV database could freely connect to and access information in the necessary databases, but these other databases would not have free access to data contained in the PIV system.

CONCERN: BACKGROUND INVESTIGATION AND ADJUDICATION

- Does the government have probable cause to do a background investigation on me?
- Is *requiring* an investigation an unlawful search and seizure?
- Are all background screeners qualified to make judgments on my eligibility for a CAC?
- How will investigators be sure they don't confuse me with another person who has the same name?
- Will I be required to tell agents everything, even past and embarrassing facts, about my life?
- Will my past mistakes cause me to be denied access to facilities?
- Will investigators base their decisions on my past history without knowing all the circumstances or mitigating factors?
- Will investigators check my credit history?
- Will credential decisions be made on credit history?
- Will extraneous circumstances be considered when credit problems exist?
- Will I be able to find out what information was used if my credential is denied?
- Will I be able to appeal a denial?

Cause for Concern

It makes sense that people do not want to be subject to unlawful investigations. People are concerned that information the government uses to make any kind of investigative decisions may be inaccurate or out-of-date or may come from a less-than-reputable source, subsequently causing a credential to be denied.

Recent reports have noted that the government uses data brokers for a number of purposes. In the wake of the February 2005 news that criminals gained access to personal identity information for about 145,000 people from the national data broker, ChoicePoint, consumers were made aware of the vast amounts of information that data brokers gather about them. They were also made aware that this information may be inaccurate and sometimes even false ("Protecting consumers' data," 2005). (For more information, see *Quality and Scope of Data Collected in Background Investigation,* p. 24.)

Example: The Transportation Security Administration (TSA) routinely compares passenger data to the FBI's terrorist watch list. Supplemental investigative data, often obtained through data brokers, are used to further identify passengers and are intended to ensure that passengers are who they claim to be. Unfortunately, this has resulted in mistaken refusal of service. Examples have been noted of individuals who have arrived at the airport to find themselves on the "no-fly" list for reasons that would not be revealed to them. Even Senator Ted Kennedy was refused service (until he had an airport supervisor identify him) because another person with a similar name was on the "no-fly" list (Goo, 2004).

Some are concerned that screeners will make security judgments without considering circumstances surrounding past crimes, poor credit history, or other personal facts that might adversely affect credential decisions. They want to know how information is used for, and more importantly, against them. Therefore, it is important that credential decisions are based on fair and impartial review of all available information, on *correct* information, and on an evaluation of the whole person, including all mitigating information and extenuating circumstances.

FIPS 201 makes it clear that all personnel will be required to undergo some form of background investigation in order to enter the PIV Program. While FIPS 201 addresses the background check requirements for various levels of sensitivity, it is not clear exactly which personnel will be subject to which specific type of background investigation. The directive gives individual agencies "enormous" discretion to conduct investigations and determine position sensitivity levels (Tien, Dixon, Pierce & Givens, 2004). Privacy advocates remain concerned that without stricter oversight for the determination of position sensitivity levels, agencies will have the opportunity to conduct unfair, unnecessary or intrusive background checks.

Additionally, FIPS 201 does not address how information from different types of investigations will be secured. For example, some personnel may be subject to credit checks, but Fair Credit Reporting Act (FCRA) requirements are not addressed. How much protection will be provided applicants with regard to their personal credit information? Will Privacy Act mandates be enough to ensure protection of personal financial and credit information?

Mitigating Facts

- In the interest of national security, the government must control who has access to federal facilities where sensitive information is stored. Therefore, the government has a legitimate reason to conduct a background investigation on any person who requires routine or ongoing access to federal facilities.
- The requirement that one must complete a background check in order to gain access to federal facilities does not constitute an unlawful search and seizure because the applicant must first provide consent for the background check. If consent is not granted, the background investigation will not be conducted, and the CAC will not be issued.
- The nature of the background check is such that it allows investigators to verify the true identity of the person through questions based on personal history. Thus, when "John Smith" is being scrutinized, investigators will make every effort to verify the information they obtain is accurate for the "John Smith" in question and is not related to any of the thousands of other persons by the same name.
- The nature of the background investigation requires most applicants to reveal facts about their lives that they may find embarrassing. In these cases, it is in the best interest of the applicant to be open and honest with investigators, even if they are embarrassed. Concealing derogatory information (lying on the security questionnaire) may be more likely to result in a credential denial than providing honest answers from the beginning.
- In accordance with the Privacy Act, individuals are legally allowed to know what information is collected, stored, and used when their credential decision is being made unless that information is part of an ongoing investigation, contains information that may violate another's privacy, or if revelation would pose a threat to national security.
- According to the due process provisions of the Privacy Act, when adverse decisions are made based on personal information, the individual in question is legally permitted to appeal the decision and ask for independent review.
- According to the FCRA, agencies must inform an applicant when an adverse decision is based on information contained in a credit report.

Considerations for Implementation

- Require background screening and security clearance for all investigators, adjudicators, and anyone else that will have access to personal information contained in this data system.
- Establish policy that only security personnel involved in the screening and adjudication processes or researchers investigating these processes have access to investigative files.
- Before any applicant is investigated and screened, set forth appropriate guidance for all investigative and adjudicative actions that will ensure fair and impartial review of all information.

  - Establish procedures for obtaining written consent from each applicant prior to the collection of any personal information or the initiation of an investigation.
  - Emphasize that applicants' written consent is required before any personal information can be collected and before an investigation can commence.
  - Decide the specific derogatory information that investigators should be looking for during the course of investigation.
  - Decide what factors may be considered derogatory and what factors are not relevant to the credential decision (refer to the Adjudicative Guidelines); these may vary for different jobs. For example, a past DUI would have very different connotations for a truck driver versus a janitor.
  - Decide what information or action is necessary to sufficiently mitigate any derogatory findings.
  - Inform applicants of these decisions in advance of their application, so that they may make an informed decision about whether to apply.
  - Provide applicants a chance to explain the circumstances surrounding any derogatory information revealed through investigation.
- Establish a systemwide policy to address investigative and adjudicative requirements for different levels of access.
- Because credit checks will be conducted for most, if not all, applicants, ensure FCRA requirements are in place before the collection of credit information begins.

CONCERN: QUALITY AND SCOPE OF DATA COLLECTED IN BACKGROUND INVESTIGATION

- Will investigators supplement the information I provide with brokered data that is known to be inaccurate?
- Will my credential decision be based on inaccurate data maintained in public records or from data broker databases?
- Can I be fired from my job based on erroneous files that have never been corrected?
- Can I be fired from my job because of past indiscretions that are revealed during my background check?
- Is the government circumventing the Privacy Act by obtaining supplemental information through data brokers?

Cause for Concern

With recent media coverage of data brokerage security breaches, Americans are more aware of the massive amounts of data that are compiled about them. Federal agencies routinely purchase brokerage files to gather information on a person.

These files are known to be riddled with errors, inaccuracies, and out-of-date information (Ramasastry, 2004; Simpson, 2001). It is very easy to link the information in a data broker's records to the wrong person, and data brokers do not routinely audit information to ensure it is true, up-to-date, or associated with the correct person. Even when an individual knows information is false, it is difficult to get the data broker to change it. False negative information can certainly have an adverse impact on a security investigation.

Examples: In 1998 a Chicago area woman was fired from her job after a ChoicePoint search incorrectly claimed that she was a convicted drug dealer and shoplifter. A Texas man was turned down for several jobs before Home Depot revealed to him that his background check with ChoicePoint identified him as a felon, which he was not. He was refused job after job based on a misdemeanor charge stemming from an incident when he was 18 years old; the incident was miscategorized as a felony. A California resident, Ron Peterson, discovered that, according to Backgroundchecks.com, he was a female prostitute in Florida, in jail for manslaughter in Texas, a dealer of stolen goods in New Mexico, and a registered sex offender in Nevada. None of these was true. These are only a few examples of mistaken identity and erroneous information that can be provided to investigators when utilizing brokered information (Zetter, 2005).

Additionally, in a routine investigative file data brokers may include information that may be personally embarrassing to a person, yet irrelevant to the security credential, such as preferred brands of consumer goods, personal habits, and private purchases.

Privacy advocates have also raised questions about the quality of data stored in federal databases. Although the Privacy Act requires databases housing personally identifying information to be kept up to date, it is possible for an agency to circumvent this requirement.

Example: The FBI's National Crime Information Center (NCIC) is a centralized database of national crime information that contains an abundance of personally identifying information. Background checks and other types of investigations routinely rely on information in the NCIC when examining an applicant's history. The NCIC was created to house data about criminal behavior. In May 2003, it was exempt from Privacy Act provisions that require administrators of government databases to regularly audit data to ensure accuracy and up-to-date information because law enforcement officials claim that in law enforcement it is difficult to know (1) if information is true or false, or (2) if information that is not currently, apparently useful will become so during the course of a future investigation.

Mitigating Facts

- Any time supplemental data are used in a personnel decision, adjudicators are expected to verify that information before using it to make a decision.

- Agencies are expected to regularly audit files containing personal information for accuracy and to ensure they are kept up to date.
- According to the Privacy Act
  - When information may be used in a way that can adversely affect a person, agencies must incorporate procedures to ensure the accuracy of data that is shared, including:
    - Allowing applicants to have access to their own data.
    - Allowing applicants to request amendment of their data.
  - Before an agency takes adverse action against an applicant based on information obtained through data sharing, it must independently verify such information before any adverse action is taken (except in cases where information is highly sensitive).
    - Agencies must provide notice to the applicant of the possibility of adverse action at least 30 days before the action is taken to give the applicant an opportunity to contest any findings.
    - Agencies must maintain all records that will be used to made a personnel decision in such a way to ensure accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure a fair decision.

Considerations for Implementation

- Consider, prior to implementation of the program, if investigators will be allowed to supplement investigative information with brokered data.
- Ensure that any supplemental investigative information that is obtained through data broker services is appropriately verified by the investigator before it is used in the investigation.
- Make a concerted effort to protect individual employees' privacy with regard to information revealed through the security investigation. This is especially important when the employee in question is not actually a government employee but an employee of a contracted entity.
- Provide applicants a chance to explain the circumstances surrounding any derogatory information revealed through investigation.
- Consider, prior to implementation of the program, how personal information can or will be used to influence an employer's or supervisor's opinion of an employee, and establish what investigative information will be shared with the employer.
- Reinforce the idea that the employer does not necessarily have a need to know all of the information revealed through the investigation.
  - Although the government has a right to ask these questions if, and only if, they are relevant to security, employers do not have a right to know if the information does not affect the employees' ability to perform their jobs.

- Information revealed through the course of investigation must be directly related to job qualifications before the employer has a right to know.
- Examples:
  - A truck driver has three DUIs in the past year—this information is relevant to the performance of the job, and therefore the employer has a right to know.
  - A truck driver likes to frequent "gay" clubs or gatherings—this information is not relevant to the performance of the job, and therefore the employer does not have a right to know if it will or could cause the employer to unfairly discriminate against the truck driver.
- Providing irrelevant information to employers, if those employers later use that information as a basis to illegally discriminate against or terminate the employee, could lead to litigation under Equal Employment Opportunity laws.

CONCERN: DATABASE CREATION AND SECURITY

- By providing my personal information, will I be contributing to the creation of a conglomeration of databases in which all information about me will be accessible?
- A database of personal information is a magnet for identity thieves.
- Are controls in place to protect against agency employees who may advertently or inadvertently reveal my personal information to someone else?
- Will I be told how my personal information will be used?
- Will my personal information be stored securely to protect against unauthorized access?
- Will the government regularly audit this database to ensure accurate and up-to-date information?

Cause for Concern

Databases can easily be linked to one another using a common identifier, such as the SSN or name. By entering the common identifier, it is relatively simple to simultaneously search numerous databases for information on a person. This is exactly what the computer programs used by data brokers, such as ChoicePoint and Acxiom, were designed to do.

People typically have two concerns about the creation of a new database that can be linked to other collections of information. First, databases are notoriously insecure. Recent and highly publicized concerns about data security in the IRS, along with data brokers ChoicePoint and LexisNexis, only help to reaffirm any concern regarding data security.

Example: Between October 2004 and April 2005, over 5 million files containing personal information were compromised, either through lost or stolen data. These security breaches at data brokers, financial institutions, universities, and retailers have made the public in general more sensitive to protecting their personal information and protecting themselves against identity theft. More importantly, the U.S. Government Accountability Office (GAO) released a report in April 2005 revealing information security weaknesses, along with an ineffective computer monitoring system, which may "impair the IRS' ability to ensure the confidentiality, integrity, and availability of its sensitive financial and taxpayer data…" (U.S. Government Accountability Office, 2005).

Second, people have a fear, be it rational or not, that an all-inclusive database will be created and used to keep "Big Brother" informed on the minute details of Americans' daily lives. This is very closely related to concerns about surveillance.

Example: The Government Accountability Office released a report in May 2004 that showed how the government uses data mining (the scouring of multiple types of data and databases in an effort to identify a pattern of abnormal behavior) to gather data on people. The same report noted GAO's concerns about privacy protections in the course of data mining, including (1) the quality and accuracy of the mined data; (2) the use of data for other than the original purpose; (3) protection of data against unauthorized access, modification, or disclosure; and (4) the right of individuals to know about data mining, how to access their information, and how to request a correction of inaccurate information (U.S. Government Accountability Office, 2004).

Mitigating Facts

- The government does not have the resources to monitor or investigate private citizens' behaviors without probable cause that a crime is occurring or has taken place.
- Agencies must publish notice in the Federal Register upon creation of a new database or upon change of an existing database, including when information from an existing database is shared or linked to another agency.
- There is certainly no ironclad protection against someone determined to compromise a computerized system. However, agencies are expected to utilize top-of-the-line technologies in securing databases.
    - According to the Privacy Act
        - Agencies are required to establish administrative, technical, and physical safeguards to ensure the security and confidentiality of personal information.
        - Agencies should appoint a senior official to oversee database security and conformity to Privacy Act requirements.

- Agencies should employ "adequate and effective security controls to protect the confidentiality, availability, and integrity of all systems and data, including all data shared with other organizations."
- When sharing information, agencies must ensure recipient agencies have adequate security controls in place before sharing information.
- Civil and criminal penalties are in place for those who violate these security rules.

- The E-Government Act requires agencies to specify when, why, and how databases containing personal information will be created and to specify administrative and technical controls that will ensure data security.
- The *National Strategy to Secure Cyberspace*[6] (Bush, 2003) recommends further actions that government agencies can take to help reduce the threat of security breaches:
  - Continuously assess threats and vulnerabilities to federal cyber systems, including agency-maintained databases housing personal information.
  - Develop agency-specific security processes:
    - Identify and document agency "architecture," including an inventory of agency operations, assets, data systems, and infrastructural links to other agencies.
    - Continuously assess threats and vulnerabilities.
    - Identify agency-specific risks and consequences related to potential attacks.
    - Implement security controls and remediation efforts to reduce and control cyber attacks.
  - Authenticate and maintain authentication for users of each system.
  - Improve security in dealing with government contractors.
  - Develop specific criteria for independent security reviews, reviewers, and certifications.
- The Privacy and E-Government Acts both require agencies to disclose how databases containing personal information will be used, both to the individuals providing the information and to the public.
- The Privacy Act requires routine audits of personal information to ensure accuracy.

[6] The *National Strategy to Secure Cyberspace* is part of the Homeland Security strategy; its purpose is to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact." For more information, see: http://www.whitehouse.gov/pcipb/

Considerations for Implementation

- Within each agency, store credential data in a single, committed database that is not accessible from outside databases without authorization.
- Establish controls to protect against the inadvertent transfer of personal information (i.e., screen outgoing e-mails for numbers formatted as SSNs; disallow "copy & paste" functions from the database to other programs).
- Require all persons with access to the database to meet strict security requirements.
- Require identity verification for all persons who wish to access the database.

CONCERN: PHYSICAL SECURITY OF PERSONAL INFORMATION

- Will my personal information be stored in a paper format?
- Will my personal information be written on or stored in my CAC in a manner that would make me vulnerable to ID theft if it were lost or stolen?
- Will my personal information be adequately destroyed when it is no longer needed?

Cause for Concern

At least one federal agency representative has expressed concern that personal information, such as pay grade and rank, might be printed on the front of the CAC, which some employees would feel was a violation of their privacy (Lee, 2004). Additionally, any personal information stored on the card, in written or electronic format, would be a cause for concern if the card were lost or stolen, therefore potentially providing the finder or thief, respectively, access to the individual's personal information and access to federal facilities.

Also, privacy advocates are concerned because FIPS 201 details the required application forms and requires that authorized identification documents (including drivers' licenses, social security cards, birth certificates, and other document containing personal identification information) be photocopied during the CAC application process. However, it provides no specification on how physical copies of personal identification documents and application forms will be secured or if records are destroyed when they are no longer needed.

Example: It is crucial that paper-based records be destroyed and not carelessly discarded in the trash. According to the 2005 Identity Fraud Survey Report, almost 60% of identity theft cases were a result of document theft (Phan, Edwards, Tariq, Woodruff, Van Dyke, Van Dyke & Neumann, 2005). Thieves are known to sort through personal residence and business mailboxes and trash in search of documents containing personal information. Others steal wallets, purses, and other personal belongings in search of drivers' licenses, Social Security cards, and credit cards that allow them to impersonate their victims.

Mitigating Facts

- Some personal information about public employees, such as pay grade and rank, is public information.
- The Government Paperwork Elimination Act was passed in an effort to reduce the collection, storage, and dissemination of paper-based information. The Act encourages the government to collect, store, and disseminate information in electronic form as often as possible.
- The Privacy Act requires that agencies have policies in place to properly destroy personal information when it is no longer needed.

Considerations for Implementation

- As often as possible, collect data electronically.
- When information is received in a physical format, convert it to electronic format as quickly as possible.
- Establish procedures for the timely destruction of paper-based information.
- When paper-based information must be stored, store it in locked file cabinets that are only accessible to persons with appropriate clearance and a direct need to know.
- Only write the minimum amount of information necessary on the front or back of the CAC.
- Encrypt information stored in the CAC so that it can only be read by authorized machines in the federal system.

CONCERN: PERSONAL CONTROL OF APPLICANT'S INFORMATION

- Can the government collect my personal information without my explicit written consent?
- Will I be able to change information I provide or that is obtained about me once it is recorded?
- Will I receive a copy of my investigation if I request one?

Cause for Concern

The government routinely investigates suspicious individuals or participates in investigations without the public's knowledge. Some Americans feel that this makes them vulnerable to unfair investigations in which they have little or no opportunity to explain and defend themselves.

Examples: Two peace activists from California are currently on TSA's "no fly" terrorist watch list. They do not know how they got on the list and cannot find information on how to get off the list, even though they have never been involved in terrorist activities (American Civil Liberties Union, 2005; "Caught in the backlash," n.d.). Over 300 San Franciscans who were on the "no fly" list were investigated by

the ACLU and *all* of them were eventually found to be free of any wrongdoing, and therefore did not belong on the list in the first place. The concern is that the ACLU had to step in before these individuals could find out anything. As individuals, they were provided no information regarding why they were on the list, what information had identified them as threats, and how they could go about correcting any misinformation (Srikantiah, 2003).

Mitigating Facts

- In accordance with the PATRIOT Act, the government does not collect personally identifying information about an individual without written consent unless that person is suspected of criminal or terrorist activity.
- All Americans have the right to "opt out" of providing their personal information. Businesses and government also have the right to refuse service (in the present case, access to facilities) to those not willing to provide information upon request.
- The Privacy Act:
  - Requires that individuals have access to read and copy any records agencies might have about them.
  - Requires an appeals process if an individual wishes to change or deny any information contained in a record.
  - Requires full disclosure as to why and for what specific purposes information is initially collected.
  - Requires that an agency obtain written permission from an individual before sharing his or her personal information with anyone else.
  - Requires a 30-day notice if information will be used to make a potentially adverse decision, so that the individual has time to appeal or provide additional information.

Considerations for Implementation

- Make sure all applicants are aware of Privacy Act provisions that allow them personal control over their information.
- Ensure efficient instructions and procedures are in place to enable applicants to review and correct information when appropriate.
- Make sure all agency representatives are aware of Privacy Act provisions and do not deny applicants rightful access to their personal information.

CONCERN: PERSONAL SECURITY

- Will my personal information be secured in a way that people who wish to do me harm (i.e., stalkers, thieves, or terrorists) will not be able to identify or locate me?

- Will people be able to identify me based on transmissions from the contactless chip embedded in the CAC?

Cause for Concern

This concern is closely related to that discussed in data security. The difference, however, has more to do with actual physical safety. Some Americans are concerned that, should a hacker obtain their personal information from a breached database, information might be used to find them. Specifically, concern exists surrounding those individuals who have worked to distance themselves from an abusive relationship or from stalkers.

Example: In Tempe, AZ, a woman was murdered by a man who found her home address in the state's DMV database. In California, a man copied the license plate numbers of five young women and used those numbers to obtain their home addresses from the DMV. He subsequently sent threatening letters to each of them (Electronic Privacy Information Center, 2004).

A related concern is that the contactless chip that will be embedded in the CAC will allow personal information to be transmitted, posing a threat to the carrier. These threats are most pronounced for Americans traveling overseas where American identification and travel documents have a high value on the black market. If an individual can be readily identified as carrying an American credential, he or she may become the target of identity thieves, foreign intelligence agents, and terrorists.

Mitigating Facts

- Personally identifying information stored in a federal agency's database is never available to the general public.
- According to rules set forth in the Privacy Act, an individual must provide written consent before personal information is released to another agency. Even then, the Privacy Act requires agencies to "keep an accurate accounting" regarding "each disclosure of a record to any person or to another agency…"
- The contactless chip will not allow identification information to be transmitted; this chip can only be read by encrypted readers at a distance of no more than 10 centimeters.
- Americans on official business overseas should always consider themselves to be a potential target and should take every precaution to protect their documentation. When traveling for personal pleasure, American travelers should leave their CACs at home.

Considerations for Implementation

- Educate people on "common sense" approaches to protecting themselves from physical threats. (i.e., Provide law enforcement brochures and other reference information when this concern arises.)

- Establish procedures that would require the individual to activate (by PIN or biometric verification) information in the CAC before it can be read by another.
- Require at least 2048 bit RSA encryption[7] in the contactless chip, which will enable information to be read only by a reader in a federal facility.

CONCERN: SURVEILLANCE

- Will the government be able to follow me wherever I go if my CAC is electronically chipped? Will they know what I buy, what I eat, etc?
- Will the government begin using my biometric information to track my day-to-day activities?

Cause for Concern

Recent concern has been expressed regarding the use of contactless microchips in identification cards. Privacy experts, and some computer experts, are concerned that contactless chips provide a means for identity thieves to access personal information and for cardholders to be covertly tracked by the "signal" of their microchip (International Civil Aviation Organization, 2004; Leach, 2004). This has led to public concern that microchips in identity documents will lead to government tracking of individual movements within and throughout buildings. Specific concern has been noted that such tracking would allow management to know when an employee has a problem or is speaking out against the administration through visits to the employee assistance program office, union office, or inspector general.

Example: Radio Frequency Identification (RFID) chips are currently used to tag consumer goods. RFID is employed as both an inventory control and purchase tracking system. It is extremely easy to track customers' purchases if they also use store loyalty cards or credit cards to pay for goods. The RFID information is electronically connected to the personal information, providing a veritable report of individual purchases. Because the RFID technology makes tracking inventory this simple, it is a logical concern that RFID would be used to track people.

Mitigating Facts

- The CAC will not be used to track individual activities outside federal facilities. The credential will only have value for access and identification when a person enters a federal system.
- The electronic chip in the CAC does not put out a signal, it only identifies a person when he or she enters a computer system, room, building, or facility, similar to the way a security guard would check an ID.
- The electronic chip in the CAC will not be connected to consumer databases and it will not allow tracking of goods and services purchased.[8]

---

[7] Commonly used 1024 bit RSA encryption has not yet been broken, but encryption experts believe that it may become breakable in the foreseeable future. Therefore, 2048 bit RSA encryption is recommended for enhanced security.

- The electronic chip used in CACs is subject to stricter security controls than the RFID technology used in consumer and inventory tracking.
- The collection and electronic storage of biometric identifiers is subject to the same laws and regulations as personal information. The Privacy Act and E-Government Act both govern the collection and storage of biometric information.
- There are no plans to use biometric information for anything other than the purposes for which they are initially collected:
  - To authenticate an applicant's identity
  - To check that identity against local, state, and federal law enforcement databases
  - To personalize the applicant's card (with a photo)
  - To electronically authenticate an individual's identity upon computer system or facility access (comparison of fingerprints to those stored)
  - To manually authenticate an individual's identity upon facility access (comparison of photo to face)

CONCERN: MISUSE OF SOCIAL SECURITY NUMBER

- Will agency employees have access to my SSN and other personal information?
- Will my SSN be used and stored on documents and in a database?
- Will I be informed when someone from another agency accesses my personal information or SSN?
- Will I be told how and when my SSN will be used?
- Will my SSN be used as my ID number?

Cause for Concern

The SSN is a universal identifier. Concern over SSN security is hardly new. Waves of identity theft have been facilitated by easy access to victims' SSNs. Americans have been repeatedly warned to protect their SSNs. Unfortunately, Americans do not have complete control over their SSNs, including who has access to them and how they are used by the agencies who store them in their databases.

A primary concern centers on agency representatives and employees who have access to SSNs. Are they trustworthy? How do we know they will not use SSNs for their own benefit? Not knowing who can access an individual's SSN is an obvious reason for apprehension when providing the SSN.

---

[8] Note: Credit and bank cards, as well as retail store loyalty cards, are routinely used to track purchases, and information is subsequently sold to data brokers. The government, however, does not sell information to data brokers or market research organizations.

Example: In 2002, a hospital clerk at Jackson Memorial Hospital in Miami, FL, stole the SSNs of 16 patients named Theresa. The clerk then provided the SSNs to a friend, also named Theresa, who opened over 200 bank and credit card accounts and made exorbitant purchases in their names (Sherman, 2002).

Additional concern stems from the fact that SSNs, like other personal information, are stored in electronic databases. It is often unclear who has access to data, and for what purposes. (See concerns on *Database Creation and Security*, p. 26, for a more detailed discussion.) While data security is a concern, the use of SSNs in such databases is also troubling. Because SSNs are considered a unique identifier, they can be used to link data across a very large range of databases and to link data within and between federal agencies and private companies (such as data brokers). (For more information, see *Third Party Access to Personal Information*, p. 17, and *Agency Sharing of Personal Information*, p. 18.)

Recently, there has been a push from both state and federal lawmakers to do away with the SSN as a personal identifier. For decades, the SSN was the enumerator of choice on drivers' licenses, student identification cards, employee identification cards, and various other forms of identification or credential. It is important for employees to know that the SSN will not be used as a primary or unique identification number, and that it will not be listed on the face of the CAC.

Mitigating Facts

- The SSN will only be available to investigators, adjudicators, and agency representatives with a legitimate purpose for seeing an individual's file.
- The SSN will be securely stored, along with other personally identifying information.
- The Privacy Act requires individuals be informed and written consent obtained when another agency or a representative of another agency requests personal information.
- The Privacy Act requires each agency to specify how personal information (including the SSN) will be used upon collection.

Considerations for Implementation

- Prescreen all employees who will have access to the SSN; require identity verification before any personnel can access a database where SSNs are stored.
- Do not stamp the SSN on the face or back of the CAC. Provide the SSN only in encrypted form in the microchip, bar code or magnetic strip.
- Encrypt the SSN in a way that it can only be "unlocked" through PIN access or biometric verification. This will ensure the card holder is aware and consenting anytime the SSN is accessed.

CONCERN: COLLECTION OF BIOMETRIC IDENTIFIERS

- Will my biometric information be stored in secure digital format?
- Will my biometric information be linked to information in other databases?
- Will providing my biometric information make me more vulnerable to ID theft?
- Will my biometric information be used for any purpose other than to verify my eligibility to access facilities?
- Are collection methods for obtaining my biometric information hygienic?

Cause for Concern

Like any personal information, biometric identifiers can be stored in a centralized database, linking them to many other databases in a way that provides a 360-degree profile of a given individual. Concern has been expressed that these same databases will subsequently be used to track purchases, transactions, preferences, and movement. As discussed previously in regard to surveillance, some fear that the government will use these technologies as a covert means of "keeping tabs" on Americans. Facial recognition is of particular concern because it can be done surreptitiously and without consent, and the individual may be given no indication that he or she is being monitored.

Example: Football fans who attended Super Bowl XXXV in Tampa, FL, were surprised and upset to learn that law enforcement officials had secretly scanned spectators' faces and compared those images to the images of known or suspected terrorists and criminals. Some felt betrayed and robbed of their perceived right to anonymity and privacy (Woodward, 2001).

Another concern related to biometrics storage is that of data security. Like any database, biometrics databases are susceptible to attack. Security breaches involving biometrics may be especially dangerous for both organizational and individual victims. If stolen, digital scans of facial images, fingerprints, and other biometrics provide thieves with potential access to secure facilities and with the tools necessary to represent another person in the least detectable way possible.

Example: At Chicago's Midway airport, a customer tried to rent a car from Dollar Rent-a-Car©, only to be informed that she must provide her fingerprints in order to rent the car. When she inquired why fingerprints were mandatory, the clerk informed her that they were used to track criminals and fraudulent renters. When asked how her prints would be disposed of, the clerk told her that they would be kept on file in Dollar's Tulsa office for at least 7 years. The customer went elsewhere because she felt providing her fingerprints for a routine service was a marked violation of her privacy. She was even more alarmed to know that Dollar did not destroy the prints once the car was returned but kept them on file for years (Amato, 2001).

Biometrics present especially difficult problems in cases of identity theft. When an identity thief uses his or her own biometrics with the name, SSN, birth date, and other information of a victim, it is sometimes impossible to distinguish the thief from the victim, thus making ID theft even more difficult to remedy.

Biometrics experts have noted that the use of biometric identifiers may evolve to be used for at least two purposes that were not originally intended. First, *unintended functional scope* refers to the use of biometric information to gain additional, and unrelated, information about the person providing the information. This occurs when information from biometric information is used to obtain detailed information that the individual may have preferred to keep private. Fingerprint malformations, for example, can indicate whether a person suffers from certain diseases or genetic disorders. Experts fear that such information may be used to covertly discriminate among people with certain physical disabilities (Prabhakar, Pankanti & Jain, 2003).

Second, *unintended application scope* refers to the identification of persons who, for lawful or reasonable purposes, intend to keep their true identity secret (Prabhakar, Pankanti & Jain, 2003). Examples include individuals in permanent or temporary witness protection who have sufficient reason to fear for their physical safety if their true identity is revealed.

A final concern relates to the sanitary collection of biometrics, both during initial collection and during scans to gain access to facilities. One specific concern is that fingerprint scanners are not kept clean enough and may subject the provider to certain diseases and illnesses ("New technologies," 2001).

Mitigating Facts

- There are no plans to use biometrics to monitor individual activities outside federal facilities.
- The biometrics embedded in the CAC will only allow tracking when an individual enters a computer system, room, building or facility, similar to the way a security guard would observe someone as he or she enters a building.
- The collection and electronic storage of biometric identifiers is subject to the same laws and regulations as personal information; The Privacy Act and E-Government Act both govern the collection and storage of biometric information. (For more information, see *Database Creation & Security*, p. 26.)
- The sharing of biometric information is subject to the same laws and regulations as sharing all personally identifying information. The Privacy Act strictly governs the sharing of personal information or the interlinking of databases. (For more information, see *Agency Sharing of Personal Information*, p. 18.)
- Biometric information is used to verify identity. Once an individual has provided his or her biometric information and identity has been verified, both with the biometric information and other sources, it becomes virtually impossible for

identity to be stolen. Certainly, no other person can claim to have the same biometrics.

- Biometric information will be collected for the following purposes:
  - To authenticate an applicant's identity.
  - To check that identity against local, state, and federal law enforcement databases in the course of the background check.
  - To personalize the applicant's card (with embedded fingerprints and photograph on the face of the card).
  - To electronically authenticate an individual's identity upon facility access (electronic comparison of fingerprints to those stored).
  - To manually authenticate an individual's identity upon facility access (human comparison of photo to face).
- It is a violation of the Americans with Disabilities Act to discriminate against a person because of a physical disability that does not hinder job performance.

Considerations for Implementation

- Only share biometric information for identity verification purposes or, when necessary, for law enforcement purposes.
- Adopt fingerprint scanning technologies that will only accept authentic fingerprint scans. New technologies reject access when silicone molds or photo-matched scans are presented and would therefore make biometric identity theft more difficult.
- Ensure that the investigative process involves an exhaustive search of persons with the same name to ensure that the applicant is not using a stolen identity. (Once biometrics are attached to a stolen identity, it is extremely difficult for the victim to recover.)
- Use biometrics only to verify identity for access to federal facilities. This will include initial identity verification during screening (including comparison checks against other federal and law enforcement databases), and identity verification upon entry to any computer system, room, building or facility.
- Be sensitive to applicants who have bona fide reasons to conceal their identity, such as those in witness protection, and work with them in an effort to ensure safety. It is expected that such situations are rare and should be dealt with on a case-by-case basis working closely with the U.S. Marshal Service.
- Establish procedures to ensure the hygienic collection of biometric information (i.e., clean fingerprint scanners in front of applicant before applicant provides biometrics; provide antibacterial hand gel or wipes for use after providing fingerprints).

DISCUSSION

This report presents an array of privacy concerns that have been voiced by Americans and discusses how these concerns relate to implementation of FIPS 201. Unfortunately, it is not possible to know every applicant's specific objections to providing personally identifying information to a government entity. Each agency should work with all PIV applicants to identify any potential concerns and to alleviate those concerns as fully as possible.

Additionally, each agency should maintain appropriate levels of awareness regarding Privacy Act and E-Government Act provisions and continually strive to protect the privacy of all personnel. Therefore, we present two policy recommendations for each agency subject to the provisions of the PIV program:

- Require annual training on Privacy Act and E-Government Act laws for all personnel involved in the collection, analysis, storage, or dissemination of personally identifying information, including data entry clerks, investigators, adjudicators, supervisors, and any other person who will have access to personal information.
- Ensure that all persons who disclose personally identifying information in the course of the PIV application process are provided a formal awareness briefing of their rights under the Privacy Act and E-Government Act.

Finally, the privacy concerns detailed in this paper are not specific only to the PIV program. Every government or corporate entity that maintains personally identifying information for any person for any purpose has a legal responsibility to protect that information and to continually ensure the safety of every individual affected. The privacy concerns and suggestions presented here are valuable for all relevant government and corporate data systems and should be aptly applied to ensure privacy protection for all Americans.

REFERENCES

Amato, T. (2001, December 21.) A fingerprint to rent a car? An ex-customer says "no." Retrieved April 12, 2005, from http://www.privacyrights.org/ar/amato.htm

American Civil Liberties Union. (2004, April 6). ACLU files first nationwide challenge to "no-fly" list, saying government list violates passengers' rights. Retrieved April 12, 2005, from http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15430&c=272

Bush, G. W. (2003, February). *National strategy to secure cyberspace*. Washington, DC: White House. Retrieved February 15, 2005, from http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Bush, G.W. (2004, August). *Homeland Security Presidential Directive/HSPD-12: Policy for a common identification standard for federal employees and contractors*. Retrieved April 12, 2005, from http://www.whitehouse.gov/news/releases/2004/08/print/20040827-8.html

Caught in the backlash: Stories from Northern California. (n.d.). Retrieved April 12, 2005, from http://www.aclunc.org/911/backlash/adams.html

Claburn, T. (2004, June 4). GAO raises privacy concerns about federal data mining. *Information Week*. Retrieved April 18, 2005, from http://informationweek.com/story/showArticle.jhtml?articleID=21401674

E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3601 *et seq.* (2002).

Electronic Privacy Information Center. (2004). *The Drivers' Privacy Protection Act (DPPA) and the privacy of your state motor vehicle record*. Retrieved April 14, 2005, from http://www.epic.org/privacy/drivers/

Goo, S.K. (2004, August 20). Sen. Kennedy flagged by no-fly list. *Washington Post*, A1. Retrieved April 10, 2005, from http://www.washingtonpost.com/ac2/wp-dyn/A17073-2004Aug19.html

New technologies in the global war on terrorism: Statement before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information. Retrieved April 14, 2005, from http://www-hoover.stanford.edu/research/conferences/nsf02/haddock.pdf

International Civil Aviation Organization. (2004). Annex I: Use of contactless ICs in machine readable travel documents. Retrieved April 14, 2005, from http://www.icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf

REFERENCES

Leach, S.L. (2004, December 9). Passports go electronic with new microchip. *Christian Science Monitor*, p. 12. Retrieved January 19, 2005, from http://www.csmonitor.com/2004/1209/p12s01-stct.htm

Lee, C. (2004, December 30). Single government ID moves closer to reality: High-tech cards are designed to bolster security. *Washington Post,* A25. Retrieved April 12, 2005, from http://www.washingpost.com/wp-dyn/articles/A35071-2004Dec29.html

Phan, D., Edwards, B., Tariq, N., Woodruff, C., Van Dyke, M.T., Van Dyke, J., & Neumann, E. (2005). *2005 Identity Fraud Survey Report*. Pleasanton, CA: Javelin Strategy & Research. One-time access complimentary copy provided by Javelin Strategy & Research Website: http://www.javelinstrategy.com/

Prabhakar, S., Pankanti, S, & Jain, A.K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy, 1*(2), 33-42. Retrieved April 12, 2005, from http://biometrics.cse.msu.edu/j2033.pdf

Protecting consumers' data: Policy issues raised by ChoicePoint: Hearing before the House Subcommittee on Commerce, Trade and Consumer Protection, Committee on Energy and Commerce, 109th Cong., 1. (2005). Retrieved April 14, 2005, from http: //energycommerce.house.gov/108/Hearings/03152005hearing1455/hearing.htm

Ramasastry, A. (2004, January 7). The safeguards needed for government data mining. Retrieved March 29, 2005, from http://writ.news.findlaw.com/ramasastry/20040107.html

REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231. (2005).

Ritchey, E.L. (2002, March 1). Et tu, school board? An essay on fingerprinting of school volunteers. *Prime Time Magazine*. Retrieved April 12, 2005, from http://www.privacyrights.org/ar/fingerprint.htm

Sherman, D. (2002, May 21). Stealing from the sick. *NBC6.net.* Retrieved July 12, 2005, from http://www.nbc6.net/news/1473178/detail.html

Simpson, G. R. (2001, April 13). FBI's reliance on the private sector has raised some privacy concerns. *The Wall Street Journal*. Retrieved March 29, 2005, from http://www.atgpress.com/privacy/pri004.htm

Srikantiah, J. (2003). The public still lacks basic information about the "no-fly" list: An analysis of TSA's FOIC response. Retrieved July 12, 2005 from http://www.aclu.org/Files/OpenFile.cfm?id=15333

Student Press Law Center. (2001). *Handout #2—SPLC legal brief: Invasion of privacy law*. Retrieved May 11, 2005, from

http://www.pbs.org/newshour/extra/teachers/lessonplans/iraq/privacy_handout.pdf

Tien, L., Dixon, P., Pierce, D., & Givens, B. (2004, December 23). *Comments on FIPS PUB 201: Personal Identity Verification (PIV) for federal employees and contractors public draft*. Retrieved April, 2005, from http://www.worldprivacyforum.org/pdf/pdffips201comments12cd23.pdf

U.S. Department of Commerce. (2005). *Personal identity verification (PIV) of federal employees and contractors* (FIPS PUB 201). Retrieved April 14, 2005, from http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf

U.S. Department of Justice. (2004a). *Overview of the Privacy Act of 1974, May 2004*. [Electronic version]. Retrieved June 22, 2004, from http://www.usdoj.gov/04foia/04_7_1.html

U.S. Department of Justice. (2004b). The Privacy Act of 1974. [Electronic version]. Retrieved June 22, 2004, from http://www.usdoj.gov/foia/privstat.htm

U.S. Government Accountability Office. (2004). *Data mining: Federal efforts cover a wide range of uses* (GAO-04-548). Retrieved April 18, 2005, from http://www.gao.gov/cgi-bin/getrpt?GAO-04-548

U.S. Government Accountability Office. (2005*). Information security: Internal Revenue Service needs to remedy serious weaknesses over Taxpayer and Bank Secrecy Act data* (GAO-05-482). Retrieved April 21, 2005, from http://www.gao.gov/cgi-bin/getrpt?GAO-05-482

U.S. Office of Management and Budget. (2000, December 20). *Guidance on interagency sharing of personal data: Protecting personal privacy* (M-01-05). Retrieved April 13, 2005, from http://www.whitehouse.gov/omb/memoranda/m01-05.html

Woodward, J.D. (2001, February 4). And now, the good side of facial profiling. *Washington Post*, B4. Retrieved April 22, 2005, from http://www.milesresearch.com/main/BiometricReferencesPreview.htm

Zetter, K. (2005, March 11). Bad data fouls background checks. *Wired News*. Retrieved April 14, 2005, from http://www.wired.com/news/privacy/0,1848,66856,00.html

OTHER RESOURCES

Agre, P.E. (2001). Your face is not a bar code: Arguments against automatic face recognition in public places. *Whole Earth, 106*, 74-77. Retrieved April 22, 2005, from http://polaris.gseis.usla.edu/pagre/bar-code.html

Alexander, L. (2005, March 30). Much as I hate it, we need a national ID. *Washington Post*. Retrieved April 8, 2005, from http://www.washingtonpost.com/ac2/wp-dyn/A11307-2005Mar29

American Civil Liberties Union. (2005, March 10). *The ChoicePoint ID theft case: What it means*. Retrieved March 24, 2005, from http://www.aclu.org/news/NewsPrint.cfm?ID=17694&c=40

Americans with Disabilities Act of 1990, 42 U.S.C.A § 12101 et seq. Retrieved April 26, 2005, from http://www.usdoj.gov/crt/ada/pubs/ada.txt

Arnone, M. (2005, March 28). IG: TSA let down privacy guard. *FCW.com*. Retrieved April 8, 2005, from http://www.fcw.com/article88409-03-25-05-Web

Association of Corporate Travel Executives. (2005, March 28). ACTE says passport "bugs" could put U.S. travelers at risk. Retrieved March 29, 2005, from http://www.acte.org/resources/press_release/032905.shtml

Biometrics technologies. (n.d.). Retrieved April, 2005, from http://www.privacyrights.org/ar/Privacy-IssuesList.htm#A

Biz execs say 'no!' (n.d.) Retrieved March 29, 2005, from http://www.rfidkills.com/execs.html

Business Travel Coalition. (2005, March 28). U.S. State Department proposed passport program is bad policy. Retrieved March 29, 2005, from http://www.becweb.biz/rfidstatement.htm

Citibank. (2004). *Citigroup privacy promise for consumers.* Retrieved May 10, 2005, from http://www.citibank.hu/privacy/index.htm

Clarke, R. (2001, April 15). *Biometrics & Privacy*. Retrieved April 22, 2005, from http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

College computer hacked, 120,000 at risk: Boston College warns alumni to watch for ID theft. (2005, March 17). *MSNBC.com*. Retrieved March 31, 2005, from http://www.msnbc.msn.com/id/7221456

ConsumerAffairs.Com. (n.d.). *Consumer complaints about Orbitz-MWI*. Retrieved April 14, 2005, from http://www.consumeraffairs.com/travel/orbitz_mwi.html

Davis v. Mississippi, 394 U.S. 721 (1969)

OTHER RESOURCES

Defense Security Service. (n.d.). *Defense Security Service Privacy Act Branch (PAB)*. Retrieved March 29, 2005, from http://www.dss.mil/contactus/privacy.htm

Defense Security Service. (2003). *Smith Amendment*. Retrieved April 26, 2005, from http://www.dss.mil/isec/dss_smith_amendment/htm

Department of the Navy. (n.d.). *PSI request procedures*. Retrieved March 31, 2005, from http://www.navysecurity.navy.mil/eff1oct03.htm

Electronic Privacy Information Center. (n.d.). *Joint letter and online petition: Require accuracy for nation's largest criminal justice database*. Retrieved March 24, 2005, from http://www.epic.org/privacy/ncic/

Electronic Privacy Information Center. (2002). *Your papers, please: From the state driver's' license to a national identification system* (Watching the Watchers Policy Report #1). Retrieved March 31, 2005, from http://www.epic.org/privacy/id_cards/yourpapersplease.pdf

Electronic Privacy Information Center. (2003a). *ENUM*. Retrieved April 14, 2005, from http://www.epic/org/privacy/enum/default.html

Electronic Privacy Information Center. (2003b). *The Privacy Act of 1974*. Retrieved April 26, 2005, from http://www.epic.org/privacy.1974act/

Electronic Privacy Information Center. (2004a). *Privacy and consumer profiling*. Retrieved April 14, 2005, from http://www.epic.org/privacy/profiling/

Electronic Privacy Information Center. (2004b). *Privacy and public records*. Retrieved April 14, 2005, from http://www.epic.org/privacy/publicrecords/

Electronic Privacy Information Center. (2005a, April 21) California considers prohibiting RFID use in state ID cards. *EPIC Alert, 12(8),* 4. Retrieved April 21, 2005, from http://www.epic.org/alert/EPIC_Alert_12.08.html

Electronic Privacy Information Center. (2005b, April 21) ChoicePoint, voter rolls and public records highlighted at CFP 2005. *EPIC Alert, 12(8),* 5. Retrieved April 21, 2005, from http://www.epic.org/alert/EPIC_Alert_12.08.html

Electronic Privacy Information Center. (2005c, April 21) Data security breaches grow in frequency, magnitude. *EPIC Alert, 12(8),* 6. Retrieved April 21, 2005, from http://www.epic.org/alert/EPIC_Alert_12.08.html

Electronic Privacy Information Center. (2005d, April 21) States and Congress to regulate data brokers in wake of scandals. *EPIC Alert, 12(8),* 2. Retrieved April 21, 2005, from http://www.epic.org/alert/EPIC_Alert_12.08.html

Friends Committee on National Legislation. (2002, February 11). *Oppose the National ID card: Letter to the President*. Retrieved March 24, 2005, from http://www.fcnl.org/issues/item_print.php?item_id=336&issue_id=80

Gellman, R. (2002). *Privacy, consumers, and cost: How the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete*. Retrieved April 14, 2005, from http://privacyrights.org/ar/gellman-email.htm

Greenemeier, L. (2005, April 6). Committee to inform Homeland Security on privacy issues. *Information Week*. Retrieved April 8, 2005, from http://www.informationweek.com/story/showArticle.jhtml?articleID=16050 1384

Greeneemeier, L. (2005, April 7). Update: Privacy committee grapples with need to know vs. need to protect. *Information Week*. Retrieved April 8, 2005, from http://www.informationweek.com/story/showArticle.jhtml?articleID=16050 2320

Keizer, G. (2005, April 20). GAO blasts IRS security, says taxpayer data vulnerable. *Information Week*. Retrieved April 21, 2005, from http://internetweek.com/security02/showArticle.jhtml?articleID=16091179 8

Laban, J. (1996). *Privacy issues surrounding personal identification systems.* State of Connecticut: Department of Social Services. Retrieved May 10, 2005, from Connecticut Department of Social Services Website, http://www.dss.state.ct.us/pubs/diprivac.pdf.

LexisNexis theft much worse than thought. (2005, April 12). *MSNBC.com*. Retrieved April 12, 2005, from http://www.msnbc.msn.com/id/7475594/print/1/displaymode/1098/

Liverpool, K. (2004). *Summary: United States Department of Justice, The Computer Matching and Privacy Protection Act of 1998 and amendments*. Unpublished manuscript.

MBNA America. (n.d.). *Privacy notice.* Retrieved May 10, 2005, from http://www.mbna.com/privacy2.html

McCullagh, D. (2003, January 13). RFID tags: Big Brother in small packages. *C/Net News.com*. Retrieved March 29, 2005, from http://news.com.com/RFID+tags+Big+Brother+in+small+packages/2010-1069_3-980325.html

McIver, R. (2005, March 22). RFID privacy issues: How RFID will impact consumer privacy. *RFiD Gazette*. Retrieved March 29, 2005, from http://www.rfidgazette.org/2005/03/rfid_privacy_is.html

OTHER RESOURCES

Merriam-Webster's dictionary of law. (1996). Springfield, MA: Merriam-Webster. Retrieved May 10, 2005, from http://dictionary.reference.com/search?q=privacy

Midgett, A. (2005, April 6). Do we deserve the freedom we have? Patriot Act up for renewal. *The Daily Reveille*. Retrieved April 12, 2005, from http://www.lsureveille.com/vnews/display.v/ART/2005/04/06/425389bf5af1d

Miller v. Murphy, 143 Cal.App.3d 337 (1983).

Millions exposed to possible ID theft: IRS security flaws put taxpayers at risk, study finds (2005, April 18). *MSNBC.com*. Retrieved April 18, 2005, from http://www.msnbc.msn.com/id/7549496

Montaldo, C. (2005). *The Patriot Act: Probable cause and due process.* Retrieved May 10, 2005, from http://crime.about.com/od/terrorism/i/partiot_act_p.htm

National Institute of Standards & Technology. (2005). *Frequently asked questions about the standard for Personal Identity Verification (PIV) of federal employees and contractors*. Retrieved April 12, 2005, from http://www.nist.gov/public_affairs/releases/piv_faqs.htm

Olsen, F. (2005, April 5). *OMB proposes ID timetable*. Retrieved April 12, 2005, from http://www.fcw.com/article88499-04-05-05-Web

Pellegrinin, F. (2002, January 8). The national ID card that isn't, yet. *Time.com*. Retrieved March 24, 2005, from http://www.time.com/time/nation/printout/0,8816,191857,00.html

Pounds, S. (2005, April 10). Identity complex: Data brokers' files are extensive, as are their destinations. *Palm Beach Post*. Retrieved April 18, 2005, from http://www.palmbeachpost.com/business/content/business/epaper/2005/04/10/a1f_data_0410.html

Privacy advocate decries ID tags in passports (2005, March 28). *GovExec.com*. Retrieved March 29, 2005, from http://www.govexec.com/dailyfeed/0305/032805tdpm2.htm

Privacy International. (2001). *Safe Harbour*. Retrieved March 24, 2005, from http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61936

Privacy Rights Clearinghouse. (2002, April 19). *Public records on the Internet: The privacy dilemma*. Retrieved March 24, 2005, from http://www.privacyrights.org/ar/onlinepubrecs.htm

Privacy Rights Clearinghouse. (2003). *"Junk" mail: How did they get my address?* Retrieved April 14, 2005, from http://www.privacyrights.org/fs/fs4-junk.htm

Privacy Rights Clearinghouse. (2004a). *Cases from the Privacy Right Clearinghouse Hotline: October 2003-September 2004*. Retrieved April 14, 2005, from http://www.privacyrights.org/cases/cases2003-2004.htm

Privacy Rights Clearinghouse. (2004b). *From cradle to grave: Government records and your privacy.* Retrieved April 14, 2005, from http://www.privacyrights.org/fs/fs11-pub.htm

Privacy Rights Clearinghouse. (2004c). *The "other" consumer reports: What you should know about "specialty" reports*. Retrieved April 14, 2005, from http://www.privacyrights.org/fs/fs6b-SpecReports.htm

Privacy? What privacy? (2004, November 22). Weblog retrieved April 14, 2005, from http://www.unix-girl.com/blog/archives/001640.html

Recent thefts of private data. (2005). *MSNBC.com*. Retrieved April 26, 2005, from http://www.msnbc.com/modules/interactive.asp?id=/d/ip/tech_databreaches_05/data.js&navid=5810485

Reuven R. R., Levary, R., Thompson, D., Kot, K., & Brothers, J. (2005, February 14). RFID, electronic eavesdropping and the law. *RFID Journal*. Retrieved April 14, 2005, from http://www.rfidjournal.com/article/articleview/1401/1/128/

Rothberger, Johnson, & Lyons, LLP. (n.d.) *Cases by category: Religious objection to government regulation.* Retrieved May 10, 2005, from http://www.churchstatelaw.com/casesbycategory.asp?category=Religious%20Objection%20to%20Government%20Regulation

Sample of opinions. (n.d.). Retrieved April 13, 2005, from http://www.ragis.com/sample.html

Sarkar, D. (2005, March 7). Privacy panel draws fire: DHS advisory group faces scrutiny for corporate-heavy membership. *FCW.com*. Retrieved April 8, 2005, from http://www.fcw.com/article88169-03-06-05-Print

Schneier, B. (2004, October 4). RFID passports. *Schneier on security: A Web log covering security and security technology*. Retrieved March 29, 2005, from http://www.schneier.com/blog/archives/2004/10/rfid_passports/html

Shopp, L. (2005, March 3). Students fall victim to Internet identity theft. *The Daily Orange*. Retrieved March 3, 2005, from http://www.dailyorange.com/news/2005/03/02/Pulp/Students.Fall.Victim.To.Internet.Identity.Theft-881955.shtml

Smart Card Alliance. (n.d.). *RFID tags, contactless Smart Card technology and electronic passports: Frequently asked questions*. Retrieved April 14, 2005, from http://www.smartcardalliance.org/alliance_activities/rfid_FAQ.cfm.

Solove, D.J., & Hoofnagle, C.J. (2005, April 5). A model regime of privacy protection 2.0: George Washington University Law School Public Law Research Paper No. 132. Retrieved April 12, 2005, from the George Washington University School of Law Website: http://www.law.gwu.edu/facweb/dsolove/PrivacyModelRegime-1-1.pdf.

Statement on government data mining before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. (2003, May 20). Retrieved March 24, 2005, from http://reform.house.gov/UploadedFiles/Steinhardt.pdf

Strohm, C. (2004, November 22). TSA to brief Congress on using commercial data for passenger screening. *GovExec.com*. Retrieved April 8, 2005, from http://www.govexec.com/story_page.cfm?articleid=29999

Sullivan, B. (2005, March 8). ChoicePoint files found riddled with errors: Data broker offers no easy way to fix mistakes, either. *MSNBC.com*. Retrieved March 31, 2005, from http://www.msnbc.msn.com/id/7118767

Support for ID cards waning. (2002, March 13). *Wired News*. Retrieved March 24, 2005, from http://www.wired.com/news/print/0,1294,51000,00.html

Thomas v. New York Stock Exchange, 306 F.Supp. 1002 (S.D.N.Y. 1969).

Tomko, G. (1998, September 15). Biometrics as a privacy-enhancing technology: Friend or foe of privacy? Paper presented at the Privacy Laws and Business 9th Privacy Commissioners'/Data Protection Authorities' Workshop, Santiago de Compostela, Spain. Retrieved April 22, 2005, from http://www.ct.gov/dss/cwp/view.asp?a=2349&q=304844

Travis, A. (2005, April 12). Passport applicants must give fingerprints: Preparation for ID cards goes ahead without parliament. *The Guardian*. Retrieved April 14, 2005, from http://www.guardian.co.uk/idcards/story/0,15642,1457297,00.html

U.S. Department of Commerce. (n.d.). *Safe Harbor overview*. Retrieved April 27, 2005, from http://www.export.gov/safeharbor.sh_overview.html

U.S. Department of Homeland Security. (n.d.). *DHS Organization*. Retrieved April 8, 2005, from http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0512.xml

U.S. Department of the Interior. (n.d.). *The Privacy Act, privacy, and you*. Retrieved April 13, 2005, from http://www.doiu.nbc.gov/orientation/privacy_act.html

U.S. Department of Justice. (2003, March 24). Rules and regulations. *Federal Register, 68*(56). Retrieved April 25, 2005, from http://www.fas.org/irp/agency/dog/fbi/is/nicipriv.html

U.S. General Accounting Office. (2003). *Electronic government: Challenges to the adoption of Smart Card technology* (GAO-03-1108T). Retrieved April, 2005, from http://www.gao.gov/new.items/d031108t.pdf

U.S. General Accounting Office. (2004). *Aviation security: Computer-Assisted Passenger Prescreening System faces significant implementation challenges* (GAO-04-385). Retrieved April 8, 2005, from http://www.gao.gov/cgi-bin/getrpt?GAO-04-385

U.S. Government Accountability Office. (2005). *Aviation security: Measures for testing the impact of using commercial data for the Secure Flight program* (GAO-05-324). Retrieved April 8, 2005, from http://www.gao.gov/new.items/d05324.pdf

U.S. Office of Management and Budget. (n.d.). *Federal agency responsibilities for maintaining records about individuals* (Appendix I to OMB circular No. A-130). Retrieved April 13, 2005, from http://www.whitehouse.gov/obm/circulars/a130/print/a130appendix_i.html

U.S. Office of Management and Budget. (2003, September 26). *OMB guidance for implementing the privacy provisions of the E-Government Act of 2002* (M-03-22). Retrieved April 13, 2005, from http://www.whitehouse.gov/omb/memoranda/m03-22.html

U.S. Office of Management and Budget. (2005). Office of E-Government and Information Technology: Notice of draft department and agency implementation guidance for Homeland Security Presidential Directive 12. *Federal Register, 70*(67), 10863. Retrieved April 13, 2005, from http://www.pubklaw.com/hi/70fr18063.pdf

U.S. Office of Management and Budget. (2005). *Instructions for complying with the President's memorandum of May 14, 1998, "Privacy and the personal information in federal records"* (Appendix I to OMB circular No. A-130). Retrieved April 13, 2005, from http://www.whitehouse.gov/omb/memoranda/print/m99-05-b.html

University Social Security numbers stolen online. (2003, March 6). *USA Today*. Retrieved March 3, 2005, from http://www.usatoday.com/tech/news/computersecurity/2003-03-06-texas-hack_x.htm

Zeller, T. (2005, March 18). Data broker curtails access to consumer details. *C/Net News.com*. Retrieved March 24, 2005, from http://msn-cnet.com.com/Data+broker+curtails+access+to+consumer+details/2100-1029_3-5625579.html?tag=mainstry